

WHAT IS CLAIMED IS:

1 1. A mobile terminal capable of identifying an
 2 authorized user, when a user connects a detachable memory
 3 medium to the mobile terminal, based on identification (ID)
 4 information stored in the memory medium, comprising:
 5 memory area creating means for creating a memory area,
 6 which is unique to each authorized user, in association
 7 with the ID information of the user;
 8 encrypting means for reading out ID information from
 9 the memory medium connected to the mobile terminal, and
 10 encrypting personal contents fed to the mobile terminal on
 11 the basis of the ID information;
 12 storing means for storing the encrypted personal
 13 contents in a specific memory area associated with the ID
 14 information; and
 15 decrypting means for reading out ID information from
 16 the memory medium connected to the mobile terminal, and
 17 decrypting, based on the ID information, the personal
 18 contents encrypted and stored in the specific memory area
 19 associated with the ID information, thereby rendering the
 20 personal contents accessible to the user.

1 2. The mobile terminal according to Claim 1, wherein:
 2 said memory area creating means automatically creates,
 3 in response to the memory medium being connected to the
 4 mobile terminal, the specific memory area in association
 5 with the ID information stored in the memory medium.

1 3. The mobile terminal according to Claim 2, wherein:
2 said memory area creating means includes means for,
3 when the memory medium is connected to the mobile terminal,
4 providing a subordinate memory area associated with the
5 specific memory area in accordance with the user's
6 operation.

1 4. The mobile terminal according to Claim 1, further
2 comprising:
3 information sharing means which allows the users at
4 least either to write contents into a common memory area,
5 which is shared by a plurality of authorized users, or to
6 gain access to contents stored in the common memory area.

1 5. The mobile terminal according to Claim 4, further
2 comprising:
3 operation means for, when the memory medium is
4 connected by the user to the mobile terminal and the
5 personal contents is accessible by the user, at least
6 either coping or transferring the personal contents to the
7 common memory area in accordance with the user's operation.

1 6. The mobile terminal according to Claim 4, further
2 comprising:
3 operation means for, when the memory medium is
4 connected by the user to the mobile terminal and the

5 personal contents is accessible by the user, at least
6 either coping or transferring information stored at the
7 common memory area to the specific memory area associated
8 with the ID information in accordance with the user's
9 operation.

1 7. The mobile terminal according to Claim 1, wherein:
2 said encrypting means generates a cryptographic key
3 based on ID information read out from the memory medium
4 connected to the mobile terminal, and encrypts personal
5 contents using the cryptographic key.

1 8. The mobile terminal according to Claim 1, wherein:
2 said decrypting means generates a cryptographic key on
3 the basis of ID information read out from the memory medium
4 connected to the mobile terminal, and decrypts the
5 encrypted personal contents stored in the specific memory
6 area associated with the ID information by using the
7 cryptographic key.

1 9. The mobile terminal according to Claim 1, wherein:
2 the ID information is a subscriber information used
3 for identifying a subscriber who is authorized to receive
4 service to be provided via the mobile terminal, or a serial
5 number uniquely assigned to the mobile terminal.

1 10. The mobile terminal according to Claim 1,

2 wherein:

3 said storing means and decrypting means dynamically
4 manage encrypted personal contents as data files having a
5 varied size in accordance with file management information
6 which makes it possible to properly manage the association
7 of ID information of individual authorized users with their
8 specific memory areas.

1 11. The mobile terminal according to Claim 1,

2 wherein:

3 the mobile terminal is shared by a plurality of users
4 and comprises a fixed specific memory area uniquely
5 assigned to each of the user;

6 said storing means, when the encrypted personal
7 contents of a user is stored in the fixed memory area
8 specifically assigned to the user, attaches a tag on a
9 header portion of the fixed memory area; and

10 said decrypting means, when it is required to decrypt
11 the encrypted personal data, determines the fixed memory
12 area specifically assigned to the user by seeking the tag
13 based on the ID information read from the memory medium
14 currently connected to the mobile terminal.

1 12. The mobile terminal according to Claim 1,

2 wherein:

3 the memory medium is an IC card based on a common
4 standard.

1 13. A method for managing information in a mobile
 2 terminal comprising a body and a memory medium with the
 3 memory medium carrying identification (ID) information
 4 being attached to or detached from the body, comprising:
 5 reading ID information from a memory medium connected
 6 to the mobile terminal;
 7 encrypting personal contents fed to the mobile
 8 terminal on the basis of the ID information, and storing
 9 the encrypted personal contents in a specific memory area
 10 associated with the ID information;
 11 reading out ID information from the memory medium when
 12 the memory medium is connected by a user to the mobile
 13 terminal; and
 14 decrypting, when the encrypted personal contents is
 15 stored in a specific memory area associated with the ID
 16 information, the encrypted personal contents based on the
 17 ID information, thereby rendering the personal contents
 18 accessible to the user.

1 14. The information management method according to
 2 Claim 13, further comprising:
 3 reading, in response to the memory medium being
 4 connected to the mobile terminal, the ID information from
 5 the memory medium; and
 6 automatically creating the specific memory area in
 7 association with the ID information.

1 15. The information management method according to
2 Claim 13, wherein:

3 in said encrypting, a cryptographic key is generated
4 on the basis of the ID information read out from a memory
5 medium connected to the mobile terminal, and the personal
6 contents fed to the mobile terminal is encrypted by using
7 the cryptographic key.

1 16. The information management method according to
2 Claim 14, wherein:

3 in said encrypting, a cryptographic key is generated
4 on the basis of the ID information read out from a memory
5 medium connected to the mobile terminal, and the personal
6 contents fed to the mobile terminal is encrypted by using
7 the cryptographic key.

1 17. The information management method according to
2 Claim 13, wherein:

3 in said decrypting, a cryptographic key is generated
4 on the basis of the ID information read out from a memory
5 medium connected to the mobile terminal, and the encrypted
6 personal contents stored in the specific memory area
7 associated with the ID information is decrypted by using
8 the cryptographic key.

1 18. The information management method according to

2 Claim 14, wherein:

3 in said decrypting, a cryptographic key is generated
4 on the basis of the ID information read out from a memory
5 medium connected to the mobile terminal, and the encrypted
6 personal contents stored in the specific memory area
7 associated with the ID information is decrypted by using
8 the cryptographic key.

1 19. The information management method according to
2 Claim 13, wherein:

3 the ID information is a subscriber information used
4 for identifying a subscriber who is authorized to receive
5 service to be provided via the mobile terminal, or a serial
6 number uniquely assigned to the mobile terminal.

1 20. A computer program for controlling an operation
2 of a mobile terminal capable of identifying, when a
3 detachable memory medium is connected to the mobile
4 terminal, an authorized user based on ID information stored
5 in the memory medium, by implementing the computer program
6 in the mobile terminal, the mobile terminal realizes:

7 a memory area creating function of creating a memory
8 area, which is unique to each authorized user, in
9 association with the ID information of the user;

10 an encrypting function of reading out ID information
11 from the memory medium connected to the mobile terminal,
12 and encrypting personal contents fed to the mobile terminal

13 on the basis of the ID information;

14 a storing function of storing the encrypted personal
15 contents in a specific memory area associated with the ID
16 information; and

17 a decrypting function of reading out ID information
18 from the memory medium connected to the mobile terminal,
19 and decrypting, based on the ID information, the personal
20 contents encrypted and stored in the specific memory area
21 associated with the ID information, thereby rendering the
22 personal contents accessible to the user.